PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-260630
(43)Date of publication of application : 29.09.1998

(51)Int.Cl. G09C 1/00
G09C 1/00
H04L 9/08

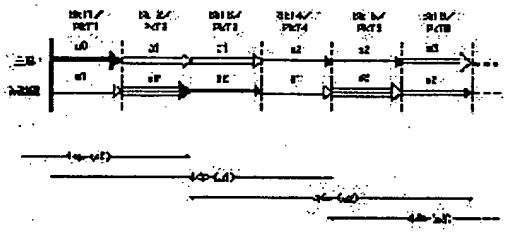
(21)Application number : 10-007018
(22)Date of filing : 16.01.1998

(71)Applicant : N T T DATA TSUSHIN KK
NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TAKAHASHI YOSHIO
MORIHATA HIDEMI

(30)Priority
Priority number : 09 6810 Priority date : 17.01.1997 Priority country : JP

(54) METHOD AND SYSTEM FOR KEY MANAGEMENT FOR ELECTRONIC SIGNATURE

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate the need to stop issuing an electronic signature at the time of update or limit the use of services after update by preparing keys used for a signature key, updating those keys according to a certain rule, and updating and making open a confirmation key in synchronism with the update of those keys.
SOLUTION: Two keys are both given an update object period of one year, a safe use period of five years, and four-year update cycles, and used as auxiliary key in the starting year and ending year and a main key in intermediate two years. Key update is performed at the start point of the final one year wherein one key is continuously the main key. At the end point of the use section of one key, the use suction of an update key is started. When the key update is performed for a key SkT for signature, a corresponding key PkT for confirmation is also updated synchronously. To issue a membership registration note, the main key for signature is used and to confirm the membership registration note, one of a pair of the main key for confirmation and an auxiliary key for confirmation is used.



LEGAL STATUS
[Date of request for examination] 18.01.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－260630

(43)公開日　平成10年(1998)９月29日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ｚ
					６３０Ｆ
		６４０			６４０Ｂ
					６４０Ｄ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｚ

審査請求　未請求　請求項の数24　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平10－7018

(22)出願日　平成10年(1998)１月16日

(31)優先権主張番号　特願平9－6810

(32)優先日　平９(1997)１月17日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　高橋　芳夫
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　森畠　秀実
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内

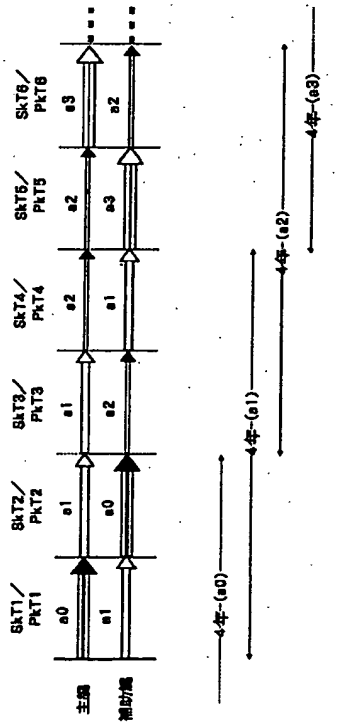
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　電子署名用の鍵管理方法及びシステム

(57)【要約】

【課題】　署名鍵を更新する際に電子署名の発行を停止したり、サービス提供を制限する必要がない、電子署名用の鍵管理方法を提供する。

【解決手段】　異なる時期に同一の更新周期で更新される２個の鍵を電子署名用の署名鍵（主鍵・補助鍵）として用意しておき、各鍵の更新周期を例えば３つの区間に分割し、更新後の最初及び最後の区間を補助鍵としての区間、中間の区間を主鍵としての区間とし、主鍵で電子署名を行う。この電子署名の確認は、署名鍵として使用されるこの２個の鍵の更新に同期して更新される２個の確認鍵のいずれかで行う。



【特許請求の範囲】

【請求項１】　各々異なる時期に周期的に内容が更新される複数の鍵を用意しておき、前記複数の鍵を、各々の鍵の更新周期よりも短い切替周期で１個づつ切り替え、切り替えた鍵を電子署名用の署名鍵としての使用に供することを特徴とする、電子署名用の鍵管理方法。

【請求項２】　前記切替周期がすべての鍵について同一長さの期間であることを特徴とする、請求項１記載の鍵管理方法。

【請求項３】　各々異なる時期に周期的に内容が更新される複数の鍵について、個々の鍵の更新周期を３つの区間に分割して最初及び最後の分割区間を予備区間、中間の分割区間を電子署名用の署名鍵として使用するための使用区間とし、各鍵についての前記使用区間を、他の鍵の使用区間と時間的に連続させ且つ互いに重複しないように切り替えることを特徴とする、電子署名用の鍵管理方法。

【請求項４】　前記署名鍵に基づく電子署名の有効期間が、前記最初の分割区間と最後の分割区間のうち短い方の区間以下の長さの期間であることを特徴とする、請求項３記載の鍵管理方法。

【請求項５】　各鍵についての前記最初及び最後の分割区間の和が当該鍵についての前記中間の分割区間と同じ長さの期間であることを特徴とする、請求項３記載の鍵管理方法。

【請求項６】　各鍵についての前記最初の分割区間と最後の分割区間とがそれぞれ同じ長さの期間であることを特徴とする、請求項３記載の鍵管理方法。

【請求項７】　一の鍵についての最後の分割区間と他の鍵についての最初の分割区間とが同じ長さの区間であることを特徴とする、請求項３記載の鍵管理方法。

【請求項８】　一の鍵についての前記使用区間中に他の鍵を更新しておき、前記一の鍵についての前記使用区間の終了時点で前記更新された他の鍵についての前記使用区間を開始させることを特徴とする、請求項３記載の鍵管理方法。

【請求項９】　前記複数の鍵の各々が、前記切り替えにかかわらず、前記署名鍵としての使用が可能なものであることを特徴とする、請求項１または３記載の鍵管理方法。

【請求項１０】　周期的に更新される第１の鍵と、この第１の鍵と異なる時期に周期的に更新される第２の鍵とを用意しておき、前記第１の鍵及び第２の鍵のいずれかを、各々の鍵の更新周期よりも短い切替周期で交互に切り替えて、電子署名用の署名鍵としての使用に供するとともに、

前記第１の鍵の更新時期に同期して更新され当該第１の鍵が署名鍵のときに確認鍵となる第３の鍵と、前記第２の鍵の更新時期に同期して更新され当該第２の鍵が署名鍵のときに確認鍵となる第４の鍵とをペアで公開し、

前記第３の鍵及び第４の鍵のペアを前記電子署名の確認用に供することを特徴とする、電子署名用の鍵管理方法。

【請求項１１】　前記第３の鍵及び第４の鍵に各々当該鍵の使用終了期限を付加することを特徴とする、請求項１０記載の鍵管理方法。

【請求項１２】　前記更新周期が、当該鍵の安全性が確保できる平均的な期間から当該鍵をもとに生成した電子署名の有効期間を減じた期間以下であることを特徴とする、請求項１、３または１０記載の鍵管理方法。

【請求項１３】　それぞれ異なる時期に周期的に更新されるＭ個（Ｍは２以上の自然数）の署名鍵を用意するとともに、個々の署名鍵の更新時期に同期して更新されるＭ個の確認鍵を同時期に公開する段階と、

前記用意したＭ個の署名鍵から１個の署名鍵を当該署名鍵の更新周期よりも短い周期で所定順に選択して所定の署名対象データの電子署名を行う段階と、

前記公開されたＭ個の確認鍵のいずれかを用いて前記電子署名を確認する段階とを含む、電子署名用の鍵管理方法。

【請求項１４】　電子署名の署名鍵として用いる複数の鍵を保持する鍵保持手段と、

前記複数の鍵の内容をそれぞれ異なる時期に周期的に更新する鍵更新手段と、

前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、

を備えたことを特徴とする、電子署名用の鍵管理システム。

【請求項１５】　電子署名の署名鍵として用いる第１の鍵及び第２の鍵を保持する鍵保持手段と、

前記第１の鍵及び第２の鍵の内容をそれぞれ異なる時期に同一周期で更新する鍵更新手段と、

前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した第１または第２の鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、

を備えたことを特徴とする、電子署名用の鍵管理システム。

【請求項１６】　前記第１の鍵に同期して更新され当該第１の鍵が署名鍵であるときの確認鍵となる第３の鍵、及び前記第２の鍵に同期して更新され当該第２の鍵が署名鍵であるときの確認鍵となる第４の鍵を保持する鍵保持手段を備え、前記第１の鍵または第２の鍵を用いて前記電子署名を行ったとときに前記第３の鍵及び第４の鍵を同時期に公開するように構成されていることを特徴とする、請求項１５記載の鍵管理システム。

【請求項１７】　前記鍵更新手段は、前記更新期間を３区間に分割するとともに、各鍵の更新を当該鍵について

の分割区間よりも短い時間内に行うように構成されていることを特徴とする、請求項１４または１５記載の鍵管理システム。

【請求項１８】　前記鍵更新手段は、一つの分割区間の鍵内容を後続の分割区間に引き継ぐ第１のモードと、直前の分割区間から後続の分割区間に移行する際に直前の分割区間の鍵内容を互いに置換する第２のモードとを選択して適用するモード選択手段とを有し、

一つの鍵について前記第１のモードを適用しているときに他の鍵の鍵内容を更新するように構成されていることを特徴とする、請求項１７記載の鍵管理システム。

【請求項１９】　前記署名手段は、前記複数の鍵の各々について、更新後の最初の分割区間の終期から最後の分割区間の始期までの間、当該鍵を電子署名用の署名鍵として用いるように構成されていることを特徴とする、請求項１７記載の鍵管理システム。

【請求項２０】　前記電子署名が会員間で会員認証に用いられる場合、前記署名手段は、前記署名対象データに、当該電子署名の有効期間と当該会員の署名確認鍵を含む個人情報とを含めて前記電子署名を行うように構成されていることを特徴とする、請求項１４または１５記載の鍵管理システム。

【請求項２１】　前記電子署名が会員間で使用可能な電子チケットの認証に用いられる場合、前記署名手段は、前記署名対象データに、当該電子チケットに基づくサービスを識別するための情報と会員の署名確認鍵とを含めて前記電子署名を行うように構成されていることを特徴とする、請求項１４または１５記載の鍵管理システム。

【請求項２２】　前記署名対象データに、当該電子チケットに基づくサービス情報の提供主体が管理する通番情報をさらに含めることを特徴とする、請求項２１記載の鍵管理システム。

【請求項２３】　Ｍ個（Ｍは２以上の自然数）の署名鍵のいずれかによって生成された電子署名と、前記電子署名に用いられた署名鍵を含むＭ個の署名鍵の更新に同期して更新されるＭ個の確認鍵を受領する署名受領手段と、

前記受領した電子署名を前記Ｍ個の確認鍵のいずれかで確認する署名確認手段とを備え、前記署名確認手段で確認がとれた電子署名を正当と判定することを特徴とする、電子署名の認証システム。

【請求項２４】　Ｍ個（Ｍは２以上の自然数）の署名鍵のうち異なる時期に更新された署名鍵によって生成された複数の電子署名と、前記複数の電子署名に用いられた署名鍵を含むＭ個の署名鍵の更新に同期して更新されるＭ個の確認鍵を受領する署名受領手段と、

前記受領した電子署名を前記Ｍ個の確認鍵のいずれかで確認する署名確認手段とを備え、前記署名確認手段で確認がとれた電子署名を正当と判定することを特徴とする、電子署名の認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子署名の発行や電子署名に基づく種々のサービスの提供等を制限することなく、電子署名用の鍵の内容を更新することを可能とする、電子署名用の鍵管理方法、及びこの鍵管理方法の実施に適したシステムに関する。ここに、電子署名とは、利用者固有の鍵を用いて利用者本人であることを証明する電子的な署名をいう。

【０００２】

【従来の技術】例えば会員証によって会員が特定される会（あるいは団体）において、会員相互で会員証の正当性を評価できるようにすることは、会の運営上、極めて重要なことである。最近は、会員証を例えばＩＣカードのような高セキュリティ性の媒体の形で発行して会員のみが所持し得る電子身分証明書としたり、オンライン上で、電子署名技術を用いて偽造の困難な会員登録証（電子身分証明書）や電子チケットとすることが試みられている。

【０００３】会員登録証や電子チケット等（以下の説明では、便宜上、会員登録証と称する）は、内容の真性評価はもとより、会員登録証を使用する者が会員本人であることを正しく確認できるようにしておくことが必要である。そのため、従来は、本人しか生成できない電子署名を用いてその会員登録証が偽造されていないかどうか、あるいは、その会員登録証の所持者が正当な会員かどうかを確認することが行われている。

【０００４】電子署名には、通常、公開鍵方式による暗号化技術が利用される。すなわち、所定の会員登録機関が自機関の秘密鍵（署名鍵）を用いて電子署名を行い、その署名鍵に対応する公開鍵（確認鍵）をすべての会員に対して配布する。各会員が電子署名の認証を行う場合は、確認鍵を用いて電子署名を確認する。なお、確認鍵自体には、会員登録機関の正当な公開鍵であることを表す情報が含まれていないので、予め確認鍵の正当性を別途確認しておく必要がある。

【０００５】上述の公開鍵方式では、安全性の根拠の一つを、解読の際の計算量の多さにおいている。従って、同一の署名鍵や確認鍵を長期間使用し続けることは安全性の低下につながるので、各鍵は、一定期間ごとに更新することが望ましい。そのため、従来は、署名鍵を定期的に更新できるようにし、その際に、署名鍵の更新に同期して更新された確認鍵を各会員が入手できるようにしているのが一般的である。

【０００６】更新された確認鍵を入手する手段としては、会員登録機関が、会員全員に新しい確認鍵を同時に配布することが考えられる。また、新しい確認鍵を所定の公開鍵証明書発行センタに登録することも考えられる。後者の場合、公開鍵証明書発行センタで、署名対象データを自己の秘密鍵（センタ秘密鍵）で署名して公開

鍵証明書とし、適宜、この公開鍵証明書を会員に配布する。配布された会員は、予め通知された公開鍵証明書発行センタの公開鍵（センタ公開鍵）で電子署名を確認する。

【０００７】ある会員が、自分の会員登録証を第三者に確認してもらいたい場合は、会員が公開鍵証明書を取得し、取得した公開鍵証明書をその会員登録証に添付する。これにより、電子署名を確認する側では、新たな会員登録機関の公開鍵の正当性を容易に確認できるようになる。なお、公開鍵証明書は、電子署名に常に添付しなければならないというものではなく、署名鍵及び確認鍵が更新されたときに１回だけ添付すれば足りるものである。

【０００８】ある会員が他の会員に対してオンラインで会員登録証を送信する場合は、送信時のデータ量を少なくするために、公開鍵証明書の添付を省略する場合がある。この場合、公開鍵証明書は、受信した会員の側で取得することになる。いずれにしても、公開鍵証明書を用いようとする場合は、確認鍵が更新される度に、会員登録証を利用する会員、あるいはその会員登録証を確認する会員が公開鍵証明書発行センタにアクセスして公開鍵証明書を取得する必要がある。

【０００９】

【発明が解決しようとする課題】上述のように、署名鍵が更新された場合は、以下のいずれかの行為が、会員登録機関と会員との間、あるいは会員相互間で行われる。

（１）会員登録機関が全会員に新しい確認鍵を配布する。

（２）ある会員が最初に会員登録証を利用する際に、公開鍵証明書を取得して添付する。

（３）電子署名を確認する会員側で、適宜公開鍵証明書を取得する。

【００１０】しかしながら、上記の三つの形態では、それぞれ下記の問題が発生する。

（１）の形態では、会員登録機関で鍵更新処理を行う場合、全利用者が一斉に新しい確認鍵を取得しようとして会員登録機関にアクセスするため、会員登録機関側に備えられるシステムにそのための処理が集中してしまい、システムの動作が不安定になるおそれがある。特に、会員数が非常に多い場合は、鍵更新後は、全利用者に新しい鍵を配布し終わるまでは会員登録証の発行を停止させなければならなくなる。

（２）の形態では、送受信の際のデータ量が増大するとともに、公開鍵証明書の取得のための時間が余分にかかる。また、公開鍵証明書が偽造されると、偽りのセンタ公開鍵が配布されてしまうので、リスクが公開鍵証明書発行センタにおけるセンタ公開鍵の安全性に依存することになる。

（３）の形態では、電子署名を確認する会員、例えばある会員の会員登録証を確認して何らかのサービスを提供しようとする会員は、ある会員の会員登録証を受信してから、公開鍵証明書を取得することになる。そのため、鍵更新後、ある会員が初めて会員登録証の確認を求める場合、公開鍵証明書を取得して会員登録証を確認するまで、当該他の会員は、サービス提供を制限するしかない。また、公開鍵証明書の取得を即時に行うために、公開鍵証明書発行センタまたは会員登録機関にオンライン・アクセスする場合には、その分、通信費が増加することになる。

【００１１】このように、従来は、署名鍵が更新される度に、いずれかのシステムの運用に悪影響を与えたり、会員のサービス利用が制限される等の不具合があった。

【００１２】本発明の課題は、上記不具合のない、電子署名用の鍵管理方法を提供することにある。本発明の他の課題は、上記鍵管理方法の実施に適したシステムを提供することにある。

【００１３】

【課題を解決するための手段】本発明の鍵管理方法は、各々異なる時期に周期的に内容が更新される複数の鍵を用意しておき、前記複数の鍵を、各々の鍵の更新周期よりも短い切替周期で１個づつ切り替え、切り替えた鍵を電子署名用の署名鍵としての使用に供することを特徴とする。前記切替周期は、例えば、すべての鍵について同一長さの期間とすることが、鍵更新を容易ならしめる上で効果的である。

【００１４】本発明の他の鍵管理方法は、各々異なる時期に周期的に内容が更新される複数の鍵について、個々の鍵の更新周期を３つの区間に分割して最初及び最後の分割区間を予備区間、中間の分割区間を電子署名用の署名鍵として使用するための使用区間とし、各鍵についての前記使用区間を、他の鍵の使用区間と時間的に連続させ且つ互いに重複しないように切り替えることを特徴とする。

【００１５】本発明の他の鍵管理方法は、周期的に更新される第１の鍵と、この第１の鍵と異なる時期に周期的に更新される第２の鍵とを用意しておき、前記第１の鍵及び第２の鍵のいずれかを、各々の鍵の更新周期よりも短い切替周期で交互に切り替えて、電子署名用の署名鍵としての使用に供するとともに、前記第１の鍵の更新時期に同期して更新され当該第１の鍵が署名鍵のときに確認鍵となる第３の鍵と、前記第２の鍵の更新時期に同期して更新され当該第２の鍵が署名鍵のときに確認鍵となる第４の鍵とをペアで公開し、前記第３の鍵及び第４の鍵のペアを、前記電子署名の確認用に供することを特徴とする。この場合、前記第３の鍵及び第４の鍵に各々当該鍵の使用終了期限を付加するようにしても良い。

【００１６】なお、前記更新周期は、当該鍵の安全性が確保できる平均的な期間から当該鍵をもとに生成した電子署名の有効期間を減じた期間以下とする。

【００１７】本発明の他の鍵管理方法は、それぞれ異な

る時期に周期的に更新されるM個（Mは２以上の自然数）の署名鍵を用意するとともに、個々の署名鍵の更新時期に同期して更新されるM個の確認鍵を同時期に公開する段階と、前記用意したM個の署名鍵から１個の署名鍵を当該署名鍵の更新周期よりも短い周期で所定順に選択して所定の署名対象データの電子署名を行う段階と、前記公開されたM個の確認鍵のいずれかを用いて前記電子署名を確認する段階とを含む。

【００１８】上記各鍵管理方法は、電子署名の署名鍵として用いる複数の鍵を保持する鍵保持手段と、前記複数の鍵の内容をそれぞれ異なる時期に周期的に更新する鍵更新手段と、前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、を備えた電子署名用の鍵管理システムによって実施可能である。

【００１９】また、電子署名の署名鍵として用いる第１の鍵及び第２の鍵を保持する鍵保持手段と、前記第１の鍵及び第２の鍵の内容をそれぞれ異なる時期に同一周期で更新する鍵更新手段と、前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した第１または第２の鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、を備えた鍵管理システムも、本発明の鍵管理方法を実施するうえで好適となる。このような鍵管理システムにおいて、好ましくは、前記第１の鍵に同期して更新され当該第１の鍵が署名鍵であるときの確認鍵となる第３の鍵、及び前記第２の鍵に同期して更新され当該第２の鍵が署名鍵であるときの確認鍵となる第４の鍵を保持する鍵保持手段をさらに備え、前記第１の鍵または第２の鍵を用いて前記電子署名を行ったとときに前記第３の鍵及び第４の鍵を同時期に公開するように構成する。

【００２０】本発明は、また、電子署名鍵と確認鍵とを受領したときに、当該電子署名が正当なものかどうかを判定することができる、電子署名の認証システムを提供する。この認証システムは、M個（Mは２以上の自然数）の署名鍵のいずれかによって生成された電子署名と、前記電子署名に用いられた署名鍵を含むM個の署名鍵の更新に同期して更新されるM個の確認鍵を受領する署名受領手段と、前記受領した電子署名を前記M個の確認鍵のいずれかで確認する署名確認手段とを備え、前記署名確認手段で確認がとれた電子署名を正当と判定することを特徴とする。署名受領手段は、M個の署名鍵のうち異なる時期に更新された署名鍵によって生成された複数の電子署名と、前記複数の電子署名に用いられた署名鍵を含むM個の署名鍵の更新に同期して更新されるM個の確認鍵を受領するように構成しても良い。この認証システムで確認がとれた場合は、当該電子署名が少なくとも本発明の鍵管理システムで生成されたことが容易にわかる。

【００２１】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。まず、本発明が適用される会員システムの概略を説明する。この会員システムは、例えば、会員のみが操作可能な複数の会員操作システムと、会員を統括管理する会員登録機関に備えられる会員登録システムと、公開鍵証明書発行センタとをそれぞれ双方向通信可能な形態、例えば図示しない通信手段を公衆網を通じて接続し、認証通信（authenticated communication）によって鍵配布を行うものである。但し、各会員操作システムと会員登録システムとの間で認証通信が可能である場合、公開鍵証明書発行センタは、必ずしも必要ではない。

【００２２】認証通信には、共通鍵方式、つまり署名鍵と確認鍵とが同一鍵である方式も採用可能であるが、以下の説明では、便宜上、前述の公開鍵方式を用いることを前提とする。

【００２３】会員登録システムは、会員からの会員登録請求情報に応じて会員登録を行う機能と、登録した各会員に対して自機関の秘密鍵（つまり署名鍵）を用いて会員登録証を発行する機能と、署名鍵を定期的に更新する機能と、署名鍵に対応する公開鍵（つまり確認鍵）を生成及び更新する機能とを有する。これらの機能の詳細については、後述する。

【００２４】公開鍵証明書発行センタは、会員登録機関名、会員登録システムが生成した確認鍵、その他の情報（署名アルゴリズムや署名の有効期間等）を署名対象データとして、自己の秘密鍵（センタ秘密鍵）で電子署名を生成し、これを公開鍵証明書として保持するとともに、この公開鍵証明書を会員からの求めに応じて適宜発行するものである。

【００２５】各会員操作システムは、会員登録システムから直接あるいは公開鍵証明書発行センタを通じて確認鍵を取得し、会員登録申請を行うものである。なお、公開鍵証明書発行センタを通じて取得する場合は、公開鍵証明書を公開鍵証明書発行センタの公開鍵（センタ秘密鍵）で確認するための処理が必要となる。

【００２６】なお、以下の説明では、システム構成やその構成要素を示す必要がある場合を除き、会員操作システムを「会員」、会員登録システムを「会員登録機関」、公開鍵証明書発行センタを「センタ」と称する。

【００２７】図１は、会員登録機関、会員、センタ間で行われる鍵、その他の電子情報の授受の様子を模式的に表した図である。センタＣＡに関する部分は、既に述べたように不可欠ではないが本例では使用する、という意味で、破線で示してある。図１において、「ＳｋＴ１」，「ＳｋＴ２」は更新前後の署名鍵、「ＰｋＴ１」，「ＰｋＴ２」は確認鍵、「ＳｋＣＡ」はセンタ秘密鍵、「ＰｋＣＡ」はセンタ公開鍵、「ＣＥＲＴ」は公

開鍵証明書、「Ｌ１，Ｌ２」は会員Ｕ１，Ｕ２に対して発行される会員登録証である。署名鍵（ＳｋＴ１，ＳｋＴ２）による電子署名は、会員登録証の発行の際に行われる。以後の説明で、会員登録証の発行という場合は、電子署名と同義とする。

【００２８】図１における鍵等の配送シーケンスは図２に示すとおりである。前提として、会員Ｕ１，Ｕ２は、センタ公開鍵ＰｋＣＡを予め取得し、公開鍵証明書を取得したときに公開鍵証明書を確認できるものとする。

【００２９】まず、会員登録機関Ｔで署名鍵ＳｋＴ１，及び確認鍵ＰｋＴ１を用意する（ステップＳ１０１）。確認鍵ＰｋＴ１については、センタＣＡに登録しておく（ステップＳ１０２，Ｓ１０３）。会員Ｕ１は、センタＣＡから公開鍵証明書ＣＥＲＴ（ＰｋＴ１）を取得した後（ステップＳ１０４）、会員登録機関Ｔに会員登録申請を行う。その際、自己の確認鍵（ＰｋＵ１）を送出する（ステップＳ１０５）。会員登録機関Ｔは、この会員の確認鍵（ＰｋＵ１）とその他の情報に対し、署名鍵ＳｋＴ１を用いて会員登録証Ｌ１を発行する（ステップＳ１０６）。

【００３０】所定期間経過後、会員登録機関Ｔでは、署名鍵ＳｋＴ１を署名鍵ＳｋＴ２に更新する（ステップＳ１０７）。そして、更新後の署名鍵ＳｋＴ２に対応する確認鍵ＰｋＴ２を、センタＣＡに再登録する（ステップＳ１０８，Ｓ１０９）。会員Ｕ２は、センタＣＡから公開鍵証明書ＣＥＲＴ（ＰｋＴ２）を取得した後（ステップＳ１１０）、会員登録機関Ｔに会員登録申請を行う。その際、自己の確認鍵（ＰｋＵ２）を送出する（ステップＳ１１１）。会員登録機関Ｔは、この会員登録申請に対し、署名鍵ＳｋＴ２を用いて会員登録証Ｌ２を発行する（ステップＳ１１２）。その後、会員Ｕ１，Ｕ２が、会員登録証Ｌ１，Ｌ２に基づく相互認証を行う（ステップＳ１１３）。

【００３１】このようにして鍵等が配送される場合において、少なくとも下記のことを行えるようにする。

（１）会員登録機関Ｔが、会員登録証の発行を中断せずに、署名鍵ＳｋＴや確認鍵ＰｋＴを定期的に更新したい。

（２）会員Ｕ１，Ｕ２間で、署名鍵ＳｋＴ１を用いて発行された会員登録証Ｌ１と、署名鍵ＳｋＴ２を用いて発行された会員登録証Ｌ２とをオフラインで正しく相互確認したい。

（３）会員登録証Ｌ１，Ｌ２の確認の際に付加情報、例えば公開鍵証明書ＣＥＲＴ（ＰｋＴ）等を相手側に送る手間を無くしたい。

【００３２】これらを解決するために会員登録機関Ｔにおいて行う本発明の鍵管理方法を、以下に説明する。まず、最も単純な例として、２個の鍵の一方を主鍵、他方を補助鍵として、両者を一定の規則に従って切り替えながら電子署名の署名鍵とし、電子署名の確認には、２個の署名鍵に対応する２個の確認鍵をペアで用いる場合の例を挙げる。つまり、署名鍵ＳｋＴ，確認鍵ＰｋＴを、それぞれ主鍵，補助鍵の２個づつ用意する。以下、説明上、主鍵と補助鍵とを区別する必要がある場合は、主鍵としての署名鍵ＳｋＴを署名用主鍵、補助鍵としての署名鍵ＳｋＴを署名用補助鍵、主鍵としての確認鍵ＰｋＴを確認用主鍵、補助鍵としての確認鍵ＰｋＴを確認用補助鍵と称する。

【００３３】各鍵は、それぞれ異なる時期に周期的に更新される。更新周期は、必ずしも同一期間である必要はない。また、各鍵には、それぞれ安全に使用できる平均的な期間（安全使用期間）が設定されており、鍵の更新周期は、当該鍵の安全使用期間から、当該鍵をもとに生成した電子署名の有効期間を減じた期間以下になるようにする。これは、鍵の解読がなされないうちに更新することで、鍵の安全性を確保しようとしたからである。なお、安全使用期間の設定は、鍵のセキュリティパラメータ、例えば鍵の長さ等を調整することによって行うことができる。電子署名の有効期間は、最初の分割区間と最後の分割区間のうち短い方の区間以下の長さの期間である。

【００３４】図３は、各鍵の更新スケジュールを具体的に示した図である。主鍵と補助鍵との関係は、署名鍵ＳｋＴ／確認鍵ＰｋＴで共通なので、一方の鍵についてのみ図示してある。ここでは、便宜上、２個の鍵の更新対象区間を共に１年、上記安全使用期間を５年、更新周期をすべて４年間隔とし、最初の１年及び最後の１年では補助鍵、中間の２年では主鍵として使用する。図中、「ａ０」，「ａ１」，「ａ３」，「ａ４」は、それぞれ鍵内容（値）である。

【００３５】図３の例の場合、各鍵について、一方の鍵の使用区間が、他の鍵についての使用区間と時間的に連続し、且つ互いに重複しないようになっている。また、補助鍵である期間の和が使用区間と同一長さの期間であり、さらに、主鍵としての最初の１年と更新前の補助鍵としての最後の１年、及び、主鍵としての最後の１年と更新後の補助鍵についての最初の１年とが同一の期間となっている。これは、主として、鍵管理の容易性を考慮したためである。鍵更新は、一方の鍵が主鍵であり続ける最後の１年の始点で行う。そして、一方の鍵についての使用区間の終了時点で、更新された鍵についての使用区間を開始させるようにする。個々の更新対象区間における主鍵及び補助鍵の内容の組み合わせは、他の区間における組み合わせと異なっている。つまり、ある更新対象区間では、ａ０とａ１、他の更新対象区間では、ａ１とａ０、あるいはａ１とａ２、・・・、となっている。

【００３６】上述の鍵更新が署名用の鍵（ＳｋＴ）についてなされた場合、それと同期して、対応する確認用の鍵（ＰｋＴ）も更新される。電子署名の生成、すなわち会員登録証の発行には、署名用主鍵を用い、電子署名の

確認、すなわち会員登録証の確認には確認用主鍵及び確認用補助鍵のペアのいずれかで行う。なお、各鍵の各々は、上記切り替えにかかわらず、署名用の鍵としての使用が可能なものである。

【００３７】上記スケジュールで鍵更新がなされ、署名用主鍵を用いて発行された会員登録証の有効期間は、最長で１年、つまり１区間分となる。従って、前述のように、２人の会員Ｕ１，Ｕ２が相互の会員登録証Ｌ１，Ｌ２を確認しようとした場合、それらは、同じ区間で発行されたものか、１個だけ前後した区間で発行されたものである。２個離れた区間で発行された会員登録証は、どちらかが有効期間が切れたものとなる。また、有効期間の重なる２個の会員登録証を所持する会員は、確認用主鍵と確認用補助鍵のどちらかを使うことで、他の会員が所持する会員登録証を確認することができる。

【００３８】また、確認用主鍵及び確認用補助鍵に当該鍵の使用終了期限を付加し、会員が他の会員の会員登録証を確認するときに、この使用終了期限が過ぎた鍵については、確認に使用しないようにすることも可能である。このようにすれば、使用終了期限の過ぎた鍵が解読されることによって行われる不正改竄にも、容易に対応できるようになる。

【００３９】なお、図３の例では、２個の鍵の更新周期がすべて４年間隔であったが、図４及び図５に示すように、２個の鍵Ａ，Ｂの更新周期がそれぞれ同一でない場合でも、本発明の鍵管理方法を実施することが可能である。

【００４０】例えば、図４の鍵更新スケジュール例では、鍵Ａ，Ｂの更新周期が５年、６年、５年、６年、・・・のように、周期的ではあるが、その周期が変化する。この例の場合、一方の鍵が主鍵として使用される区間で他方の鍵が補助鍵となる点は図３の例と同様であるが、各鍵についての使用区間が必ずしも一定ではない点が異なる。つまり、５年中２年の場合もあれば、５年中３年である場合もある。しかし、この場合も、一方の鍵を、他方の鍵が主鍵であり続けるうちに更新しておき、他方の鍵についての使用区間が終了した時点で更新後の鍵（それまでは補助鍵）についての使用区間を開始させるようにすることで、鍵更新をスムーズに行うことができるようになる。また、個々の鍵についての安全使用期間を上記更新周期よりも長くし、且つ電子署名の有効期間を、署名用主鍵として使用可能になった時点から１年以下とすることで、鍵の使用上のセキュリティも確保することができる。この場合の確認鍵も、確認用主鍵、確認用補助鍵のペアで公開し、確認者がペアの確認鍵のいずれかを用いて電子署名を確認できるようにする。

【００４１】図５の鍵更新スケジュール例では、鍵Ａの更新周期が５年、６年、５年、６年、・・・、鍵Ｂの更新周期が５年、５年、６年、６年、・・・のように周期が変化する。この場合も上記同様の規則に従って鍵更新を行い、主鍵と補助鍵とを交互に切り替えることで、図３及び図４の例と同様の効果を期待することができる。

【００４２】また、上述の例では、署名用及び確認用の鍵を２個づつ用意した場合の例であるが、本発明の鍵管理方法は、鍵が３個以上であっても実施することが可能である。例えば、５つの鍵を用いた場合の鍵更新スケジュール例を図６に示す。図６の例では、便宜上、５つの鍵Ａ～Ｅがすべて５年周期で更新され、それぞれ１年毎に主鍵に切り替わるようにしている。つまり、補助鍵として使用する期間は、それぞれ使用区間（１年）の前後２年となる。各鍵Ａ～Ｅの安全使用期間を７年以上とすれば、電子署名の有効期間は最大で２年とすることができ、図３の例（鍵が２個の場合）の有効期間（１年以下）よりも長くすることができる。

【００４３】図６の鍵更新スケジュール例の場合、電子署名を生成した後、確認用に同時期に公開する確認鍵は、最大で５つとなる。この５つの確認鍵のいずれかを用いて電子署名を確認することができる点は、図３の例の場合と同様である。なお、各鍵Ａ～Ｅの更新周期を、必ずしも同一長さとしなくとも良いことは、前述のとおりである。

【００４４】次に、上記鍵管理方法を実施するための鍵管理システムについて説明する。この鍵管理システムは、会員システムの個々の機関、例えば前述の会員登録機関Ｔに、単独あるいは分散して備えられるもので、図７に示すように、演算処理装置１，表示出力装置２、データ入出力装置３、通信網接続装置４，情報処理制御部５，データファイル装置６，時間管理装置７，及び鍵生成装置８を有している。

【００４５】演算処理装置１は、図示しない外部記憶装置やＲＯＭに記録されたプログラムを実行することで所要の機能を実現する一種のコンピュータであり、表示出力装置２は、演算処理装置１等による処理結果を視覚化するディスプレイ装置である。データ入出力装置３は、マウスその他のポインティングデバイスやキーボード等、外部記憶装置、及びこれらとの間のインタフェースを含むものである。通信接続装置４は、種々の会員やセンタＣＡとの間で行う通信を制御するものである。時間管理装置７はタイマ、鍵生成装置８は、鍵を生成する装置である。

【００４６】情報処理制御部５は、例えば演算処理装置１が上記プログラムを読み込んで実行することにより形成される機能ブロックであり、図８（ａ）に示すように、モード更新の契機を付与する契機付与処理部５１と、モード更新を行う更新処理部５２と、主鍵・補助鍵の入れ替えを行う入れ替え処理部５３と、主鍵・補助鍵の鍵内容を置換する置換処理部５４と、電子署名を行う生成部５５と、電子署名や主鍵・補助鍵を外部へ送信する送信処理部５６とを有している。

【００４７】契機付与処理部５１では、一つの分割区間

の鍵内容を後続の分割区間に引き継ぐモードＡと、直前の分割区間から後続の分割区間に移行する際に鍵内容を互いに置換するモードＢとを選択的に適用するための契機を出力する。図３の鍵更新スケジュールに示した例では、１年が経過して２年目に移行する際にモードＢが適用され、鍵内容ａ０，ａ１が主鍵・補助鍵で相互に置換される。２年目が経過して３年目に移行する際にモードＡが適用され、主鍵の鍵内容ａ１は引き継がれるが、補助鍵の鍵内容ａ０は、「ａ２」に更新される。モードＡとモードＢは周期的に適用されるため、以下の説明では、モードＡ後、モードＢが適用されるまでのサイクルをサイクルＡ、モードＢ後、モードＡが適用されるまでのサイクルをサイクルＢと称する場合がある。

【００４８】更新処理部５２は、上述のモード切換を行い、現在のサイクルを表すモードフラグ（サイクルＡ／Ｂ）をデータファイル装置６に記録しておき、以後のモード更新時（サイクル切替時）に参照できるようにしておく。入れ替え処理部５３は、署名鍵及び確認鍵の各々について、主鍵と補助鍵とを入れ替えるものであり、置換処理部５４は、鍵内容を新しいものに置換するものである。生成部５５は、署名用主鍵を用いて、署名生成要求毎に指定された署名対象データの電子署名を行うものである。

【００４９】データファイル装置６は、図８（ｂ）に示すように、モードフラグ６１、確認用主鍵６２、署名用主鍵６３、確認用補助鍵６４、署名用補助鍵６５がそれぞれ格納されている。会員登録機関Ｔが確認用主鍵６２と確認用補助鍵６４を保持するのは、センタＣＡによらず、直接会員に確認鍵を配布する場合があるためである。

【００５０】次に、上記鍵管理システムを応用した会員システムの運用形態を説明する。この会員システムは、図９の概略図に示すように、それぞれ会員であるチケット販売機関Ｂ、利用者会員Ｕ、サービス提供者Ｉを、通信網を通じて会員登録機関Ｔに接続して構成される。本発明の鍵管理システムは会員登録機関Ｔに設けられるが、他の会員も同時に備えるように構成してもよい。各会員は、少なくとも暗号技術を用いた認証通信が可能であるものとする。この会員システムの運用手順は、図１０～図１２に示すとおりである。

【００５１】（１）会員登録

図１０を参照し、会員登録機関Ｔは、まず鍵の更新を行う日を設定する（例えば、毎年１月１日）。また、確認用主鍵ＰｋＴｍ６２、署名用主鍵ＳｋＴｍ６３と、確認用補助鍵ＰｋＴｓ６４、署名用補助鍵ＳｋＴｓ６５を用意し、モードフラグ６１を「サイクルＡ」に設定する（ステップＳ２０１）。利用者会員Ｕは、自らの署名鍵ＳｋＵと確認鍵ＰｋＵとを作り、確認鍵ＰｋＵと利用者名などの会員情報ＩｄＵとからなる会員登録請求情報を会員登録機関Ｔへ送信する（ステップＳ２０２）。

【００５２】会員登録機関Ｔでは、この送信された会員登録請求情報から確認鍵ＰｋＵを抽出して、鍵管理システムの生成部５５により、これに有効期限Ｅｌｕをつけたものを署名対象データとする。そして、署名用主鍵ＳｋＴｍを用いてこの署名対象データに署名して会員登録証Ｌｕを発行する。その後、送信処理部５６により、会員登録証Ｌｕを、有効期限Ｅｌｕ、確認鍵ＰｋＵ、会員情報ＩｄＵ、及び前述の確認用主鍵ＰｋＴｍ６２、確認用補助鍵ＰｋＴｓ６４と共に、利用者会員Ｕへ送信する（ステップＳ２０３）。

【００５３】会員登録機関Ｔは、会員登録の請求をいつでも受付可能にすることができて、会員登録の日から１年間有効な会員登録証Ｌｕを発行する。チケット販売機関Ｂ、サービス提供者Ｉも、同様にして、会員登録を行い、会員登録証Ｌｂ，Ｌｉの発行を受ける。

【００５４】１回目の鍵更新の日（１月１日）が到来すると、会員登録機関Ｔは、モードフラグ６１を参照し、更新処理部５２で現在のサイクルＡをサイクルＢに更新する（ステップＳ２０４）。続いて、入れ替え処理部５３で、主鍵と補助鍵とを入れ替える（ステップＳ２０５）。

【００５５】２回目の鍵更新の日（翌年の１月１日）が到来すると、会員登録機関Ｔは、更新処理部５２で現在のサイクルＢをサイクルＡに更新する（ステップＳ２０６）。続いて、鍵生成装置８で生成した新しい鍵を、置換処理部５４で補助鍵として保存する（ステップＳ２０７）。これを更新周期である４年間の間に、もう１サイクルずつ繰り返す（ステップＳ２０８～Ｓ２１１）。

【００５６】利用者会員Ｕ、チケット販売機関Ｂ、サービス提供者Ｉへの確認用の鍵の配布（確認用主鍵ＰｋＴｍ６２，確認用補助鍵ＰｋＴｓ６４の送信）は、安全のためにオフラインでの処理を含めることが望ましい。例えば、対面で手渡しするとか、郵送や、ファクシミリなどで送るなどの方法を併用すると、より安全になる。オンラインでのみ行う場合は、何等かの認証通信を行う必要がある。センタＣＡの公開鍵証明書を利用する場合、通常の公開鍵証明書には、公開鍵である確認鍵は１個しか含まれないため、公開鍵証明のフォーマットを修正して公開鍵を２個含めるようにする方法と、公開鍵証明書を２個利用する方法がある。これによって、センタＣＡの公開鍵証明書を利用することができる。

【００５７】（２）サービス提供情報の登録

図１１を参照し、サービス提供者Ｉは、サービス提供保証情報Ｃ、チケット販売機関Ｂの確認鍵ＰｋＢ、サービスの有効期限Ｅｃ、チケットの発行通番Ｒｃ、会員情報ＩｄＩ、その他サービス内容・金額など、必要に応じた項目情報をチケット販売機関Ｂへ送信する（ステップＳ３０１）。これは、サービス提供者Ｉが、事後的に送られたチケットの真偽を事後的に確認できるようにする情報である。このような情報を予めチケット販売機関Ｂに

登録しておくことで、利用者会員Ｕによるチケットの２重使用や、チケット販売機関Ｂが不正した場合に、サービス提供前に、検出可能になるというメリットがある。

【００５８】（３）チケットの販売

利用者会員Ｕとチケット販売機関Ｂとの間で、相互に会員登録証Ｌｕ，Ｌｂを確認する場合は、次のような手順となる。利用者会員Ｕは、まず、会員登録証Ｌｕ，確認鍵ＰｋＵ、有効期限ＥｌＵ、及びチャレンジ（認証依頼）を、チケット販売機関Ｂへ送信する（ステップＳ３０２）。ここではチャレンジは、暗号化技術・署名技術の一例として使用されている。

【００５９】チケット販売機関Ｂは、利用者会員Ｕから送られてきた会員登録証Ｌｕ等を、自分の保管している確認用主鍵ＰｋＴｍ・確認用補助鍵ＰｋＴｓの両方で試す（ステップＳ３０３）。利用者会員Ｕの会員登録証Ｌｕと、チケット販売機関Ｂの会員登録証Ｌｂは、どちらが先に発行されたものであっても、また、先の発行と後の発行との間に、会員登録機関Ｔが、署名鍵を更新した場合であってもよい。両方とも有効な会員登録証Ｌｕ，Ｌｂである限り、どちらか片方の確認鍵で、署名の確認ができる。公開鍵証明書発行センタＣＡに公開鍵証明書を取りにいったり、利用者から送信する必要はない。どちらか片方の確認鍵で、署名の確認ができたら、次の処理に進む。確認できなかった場合は、会員登録証Ｌｕが有効ではないことを意味するので、チケットの販売を拒否する（ステップＳ３０４：No、Ｓ３０５）。

【００６０】次に、チケット販売機関Ｂは、自分の会員登録証Ｌｂ、確認鍵ＰｋＢ、有効期限ＥｌＢ、及び利用者会員Ｕから送られてきたチャレンジに対して、チケット販売機関Ｂの署名鍵ＳｋＢを用いて生成した署名を利用者会員Ｕへ送信する（ステップＳ３０６）。利用者会員Ｕは、チケット販売機関Ｂから送られてきた会員登録証Ｌｂを、自分の保管している確認用主鍵ＰｋＴｍ・確認用補助鍵ＰｋＴｓの両方で試す（ステップＳ３０７）。どちらか片方の確認鍵で、署名の確認ができたら、次の処理に進む。確認できなかった場合は、会員登録証Ｌｂが有効ではないことを意味し、偽りのチケット販売機関である可能性があるので、購入を取り止める（ステップＳ３０７：No、Ｓ３０８）。

【００６１】会員登録証Ｌｂの確認ができたら、自分の送ったチャレンジに対するチケット販売機関Ｂの署名をチケット販売機関Ｂの確認鍵ＰｋＢで確認する。確認できた場合は、次に進む。なお、確認鍵ＰｋＢがチケット販売機関Ｂの正当な公開鍵であることは、チケット販売機関Ｂの会員登録証Ｌｂを確認することで確認されている。利用者会員Ｕは、購入したいチケットの情報Ｈにチケットの情報とチケット販売機関Ｂが生成したチャレンジに対する利用者会員Ｕの署名鍵にて生成した電子署名を添付して、チケット販売機関Ｂへ送信し、チケットの購入を申し込む（ステップＳ３０９）。

【００６２】チケット販売機関Ｂは、利用者会員Ｕから送られてきたチケット情報とその電子署名を、利用者会員Ｕの確認鍵ＰｋＵにて確認する（ステップＳ３１０）。チケット情報とその電子署名の確認ができた場合は、次の処理に進む（ステップＳ３１１：Yes）。確認できなかった場合は、会員登録証Ｌｕの正当な所持者以外のものが購入の申込みをしているか、通信中にデータが改竄されていることを意味するので、チケットの販売を拒否する（ステップＳ３１１：No、Ｓ３１２）。

【００６３】チケット販売機関Ｂは、また、利用者会員Ｕの確認鍵ＰｋＵ、サービス提供保証情報Ｃ、有効期限Ｅｃ、発行通番Ｒｃ、会員情報ＩｄＩ、チケット販売機関Ｂのチケット販売通番Ｒｆ、及びチケット有効期限Ｅｆを合わせたものを署名対象データとして、チケット署名情報Ｆを生成する。ここでチケット署名情報Ｆは、チケット毎に別々の値にならなければならないため、署名対象データにチケット販売通番Ｒｆを含めるようにする。その後、サービス提供者Ｉの会員登録証Ｌｉ、確認鍵ＰｋＩ、及び有効期限ＥｌｉＩと、チケット販売通番Ｒｆ、チケット有効期限Ｅｆ、及びチケット署名情報Ｆを利用者会員Ｕへ送信する（ステップＳ３１３）。

【００６４】利用者会員Ｕは、サービス提供者Ｉの会員登録証Ｌｉを会員登録機関Ｔの確認鍵ＰｋＴでチェックする。会員登録証Ｌｉの確認ができた場合は、サービス提供者Ｉの確認鍵ＰｋＩで上記サービス提供保証情報Ｃを確認し、さらに、チケット販売機関Ｂの確認鍵ＰｋＢで上記チケット署名情報Ｆを確認する。チケット署名情報Ｆ等の確認ができた場合は、料金＄の支払いを行う（ステップＳ３１４）。

【００６５】（４）チケットの使用

図１２を参照し、利用者会員Ｕは、会員登録証Ｌｕ、確認鍵ＰｋＵ、有効期限Ｅｌｕとチャレンジをサービス提供者Ｉへ送信する（ステップＳ４０１）。サービス提供者Ｉは、チケット販売機関Ｂと同様に利用者会員Ｕの会員登録証Ｌｕを確認する（ステップＳ４０２）。確認できた場合は、サービス提供者Ｉの会員登録証Ｌｉ、チャレンジに対する電子署名、及びチャレンジを利用者会員Ｕへ送信する（ステップＳ４０３：Yes、Ｓ４０５）。

【００６６】利用者会員Ｕもサービス提供者Ｉの会員登録証Ｌｉを確認し、チャレンジの電子署名を確認する（ステップＳ４０６）。確認できた場合（ステップＳ４０７：Yes）、利用者会員Ｕは、チケット署名情報Ｆとサービス提供者Ｉの確認鍵とチャレンジを合わせたものに、自分の署名鍵で、利用者署名情報Ｓ、会員登録証Ｌｂ、確認鍵ＰｋＢ、有効期限ＥｌｂＩ、チケット署名情報Ｆ、チケット販売通番Ｒｆ、有効期限Ｅｆ、サービス提供保証情報Ｃ、発行通番Ｒｃ、有効期限Ｅｃ、会員情報ＩｄＩの電子署名を生成して、サービス提供者Ｉへ送信する（ステップＳ４０７：Yes、Ｓ４０９）。

【００６７】サービス提供者Ｉは、サービス提供保証情報Ｃ、チケット署名情報Ｆ、利用者署名情報Ｓ、チケット有効期限Ｅｆ，Ｅｃ、及びチケットが既にしようされていないかどうかを確認する。確認できた場合は、サービス提供を開始する（ステップＳ４１０）。サービス提供者Ｉ、利用者会員Ｕの相互認証の結果が否定的であった場合は、サービス提供や申し込みが拒否される（ステップＳ４０３：No，Ｓ４０４、Ｓ４０７：No、Ｓ４０８）。

【００６８】（５）チケットの譲渡

また、会員間で、次のようにやり取りすることで、チケットの譲渡をすることも可能である。会員Ｕ１は、チケットに譲渡証明を示す署名をつけて、会員Ｕ２に渡す。会員Ｕ２は、チケットと譲渡証明を、サービス提供者Ｉへ送信する。サービス提供者Ｉは、チケットと譲渡証明とを確認して、会員Ｕ２にサービスを提供する。

【００６９】なお、会員システムを運用する場合において、利用者会員Ｕが提示した会員登録証が、会員登録機関Ｔから発行されたものかどうか、あるいは電子署名が正当かどうかを、上記チケット販売機関Ｂやチケット提供者Ｉとは別に、確認する必要が生じる場合がある。この場合は、本発明の認証システムを用いて当該会員登録証の正当性を確認する。この認証システムは、電子署名と複数の確認鍵とを受領してその内容を確認する第１の確認処理部と、受領した電子署名を複数の確認鍵のいずれかで確認する第２の確認処理部とを備え、第２の確認処理部で確認がとれた場合は、その電子署名が正当なものと判定する。これらの確認処理部は、例えばコンピュータが所定のプログラムを読み込んで実行することによって当該コンピュータ内に形成される機能ブロックである。なお、受領した電子署名は、異なる時期に更新された署名鍵によって生成されたものであっても良い。

【００７０】次に、図１３を参照して、会員システムの他の構成例を示す。基本的な動作は図９に示した構成の会員システムと同様であるが、ここでは、本発明の鍵管理システムを、会員登録機関Ｔのほか、チケット販売機関Ｂにも設けている。また、図９に示した構成の会員システムでは、チケット販売機関Ｂの鍵は１組であるが、ここでは、２組の鍵でもって会員登録証Ｌの発行を請求するようにする。

【００７１】すなわち、チケット販売機関Ｂでは、チケット用の署名鍵（ＳｋＢｍ／ＳｋＢｓ：以下、チケット署名鍵）を主鍵と補助鍵の２個用意し、これを、例えば図３に示したような鍵管理スケジュールで更新するようにする。なお、会員登録証Ｌの更新契機とチケット署名鍵の更新契機は、同一である必要はないが、同一でも構わない。但し、チケット署名鍵は、会員登録証Ｌの有効期間と同じかそれ以上の有効期間をもつことが必要である。ここでは、会員登録証Ｌの更新契機で、当該会員登録証Ｌと同じ長さの有効期間を持つチケット署名鍵を使用する。例えば、４月１日に会員登録することにして、１年毎に更新を行うこととする。

【００７２】チケット販売機関Ｂの会員登録証Ｌｂの有効期限ＥＩｂが切れたとき、そのときのチケット販売機関Ｂの確認鍵ＰｋＢｍ／ＰｋＢｓを会員登録機関Ｔに送り、新たな会員登録証Ｌｂを発行してもらう。サービス提供者Ｉは、サービス提供保証情報Ｃをチケット販売機関Ｂに預けるのを契機にして、チケット販売機関Ｂの会員登録証Ｌｂと、確認鍵ＰｋＢｍ／ＰｋＢｓと、有効期限ＥＩｂとを入手する。サービス提供保証情報Ｃの有効期限Ｅｃは、例えば発行後１年以下とする。会員登録証Ｌｂの署名を確認できたら、会員登録証Ｌｂ、確認鍵ＰｋＢｍ／ＰｋＢｓ、及び有効期限ＥＩｂを保管する。

【００７３】利用者会員Ｕは、チケットの購入を契機にして、チケット販売機関Ｂの会員登録証Ｌｂを入手する。ここで入手したチケット販売機関Ｂの会員登録証Ｌｂは、チケットの確認後は、保管する必要がなくなることが、チケット販売機関Ｂに、本発明の鍵管理システムを用いた場合のメリットの一つである。

【００７４】利用者会員Ｕは、チケットを、サービス提供者Ｉへ送信する。ここでは、サービス提供保証情報Ｃ、チケット署名情報Ｆ，利用者署名情報Ｓ，会員登録証Ｌｕ、有効期限Ｅｃ、発行通番Ｒｃ、会員情報ＩｄＩ、チケット販売通番Ｒｆ、有効期限Ｅｆ、確認鍵ＰｋＵ、有効期限ＥＩｕを送信することになる。サービス提供者Ｉは、チケット販売機関Ｂの会員登録証Ｌｂを入手した後、利用者会員Ｕが、チケット販売機関Ｂの署名を入手するまでの間に、サービス提供者Ｉの鍵の更新が行われた場合でも、チケット販売機関Ｂの主鍵か補助鍵のどちらかで、会員登録証Ｌｂを確認することができるので、再度鍵を取得する処理を行う必要はない。

【００７５】次に、鍵更新スケジュールについて説明する。この場合も会員登録機関Ｔは、１年毎に鍵を更新するものとする。但し、上述したように、会員登録機関Ｔは、５年間有効の１個の鍵を２年毎に生成するものであり、この１個の鍵は、最初と最後の区間、すなわち１年目と４年目の区間で補助鍵として使用し、その間の２区間、すなわち２年目と３年目の区間で主鍵として使用する。このとき、会員登録証の有効期間は１年間、若しくは１年未満とする。チケット販売機関Ｂは、会員登録機関Ｔとは異なるタイミングで鍵の更新を行う。このときの周期は同じ１年毎とする。また、チケット署名情報Ｆの有効期間は１年間、若しくは１年未満とする。

【００７６】会員登録機関Ｔとチケット販売機関Ｂは、それぞれ鍵を更新すると、これをセンタＣＡに登録する。これは、認証通信の代用とするためである。このようにセンタＣＡへ登録する場合、利用者会員Ｕ及びサービス提供者Ｉは、会員登録証Ｌの更新や、サービス提供保証情報Ｃの登録や、チケット署名情報Ｆの購入を契機に、会員登録機関Ｔやチケット販売機関Ｂの鍵をセンタ

ＣＡから取得できるようになる。

【００７７】以下、実際の鍵更新の様子を図１４のスケジュール例に従って説明する。ここでは、サービス提供保証情報Ｃの預入時にサービス提供者Ｉとチケット販売機関Ｂとの間で、チケットの購入時に利用者会員Ｕとチケット販売機関Ｂとの間で、チケット使用時に利用者会員Ｕとサービス提供者Ｉとの間で、それぞれ会員登録機関Ｔが発行した会員登録証が確認でき、かつチケットの使用時に、チケット販売機関Ｂが発行したチケット署名情報Ｆが確認できることを要点とする。

【００７８】図１４では、最初の区間（１年目）での確認鍵ＰｋＴ１の内容は、主鍵がｔｏ、補助鍵がｔ１であるとする。２番目の区間での確認鍵ＰｋＴ２は、主鍵と補助鍵とが入れ替えられ、主鍵はｔ１、補助鍵はｔｏとなる。さらに、３番目の区間での確認鍵ＰｋＴ３は、主鍵はｔ１のまま、補助鍵は新しく生成された内容ｔ２となる。

【００７９】利用者会員Ｕの会員登録証Ｌ１は、３番目の区間で発行される。具体的には、当該区間での確認鍵ＰｋＴ３の主鍵ｔ１に対応する署名鍵ＳｋＴ３の主鍵で生成される。このとき、当該区間での確認鍵ＰｋＴ３の主鍵ｔ１と補助鍵ｔ２とが利用者会員Ｕに配布される。また、会員登録証Ｌ２は、４番目の区間で発行される。具体的には、当該区間での確認鍵ＰｋＴ４の主鍵ｔ２に対応する署名鍵ＳｋＴ４の主鍵で生成される。このとき、確認鍵ＰｋＴ３の主鍵ｔ２，補助鍵ｔ１が利用者会員Ｕに配布される。サービス提供者Ｉの会員登録証Ｌ１、Ｌ２，Ｌ３，．．．、チケット販売機関Ｂの会員登録証Ｌ１、Ｌ２，Ｌ３，．．．、についても同様である。但し、ここではチケット販売機関Ｂの鍵も本発明の鍵管理方法で鍵更新を行っている。図１４でチケット販売機関Ｂの横に記載されているＰｋＢ１，ＰｋＢ２，．．、の部分は、このことを意味している。チケット販売機関Ｂは、主鍵と補助鍵を合わせた確認鍵を、会員登録機関Ｔに送り、会員登録証を発行してもらう，

【００８０】次に、利用者会員Ｕとサービス提供者Ｉとの間の認証について説明する。利用者会員Ｕの会員登録証Ｌ２は、ｔ１の署名鍵で発行されている。それと重なる有効期間を持つサービス提供者Ｉの会員登録証Ｌ２は、発行時に、主鍵ｔ１，補助鍵ｔ２を取得しているため、利用者会員Ｕの会員登録証Ｌ１を主鍵ｔ１で確認することができる。また、サービス提供者Ｉの会員登録証Ｌ２は、主鍵ｔ２，補助鍵ｔ１を取得しているため、今度は利用者会員Ｕの会員登録証Ｌ１の署名内容を補助ｔ１で確認することができる。

【００８１】逆に、利用者会員Ｕは、会員登録証Ｌ１の発行時に主鍵ｔ１，補助鍵ｔ２を取得しているため、主鍵ｔ１で生成されているサービス提供者Ｉの会員登録証Ｌ１や、主鍵ｔ２で生成されている会員登録証Ｌ２を確認することができる。利用者会員Ｕは、また、会員登録証Ｌ２の時は、主鍵ｔ２、補助鍵ｔ１を取得しているため、主鍵ｔ２にてサービス提供者Ｉの会員登録証Ｌ２を確認することができる。サービス提供者Ｉとチケット販売機関Ｂ、利用者会員Ｕとチケット販売機関Ｂについても同様に確認を行うことができる。

【００８２】このように、会員登録証の発行はいつでも行うことができ、また、サービス提供者Ｉとチケット販売機関Ｂ、利用者会員Ｕとチケット販売機関Ｂ、利用者会員Ｕとサービス提供者Ｉ　との間で、お互いの会員登録証Ｌが有効である限り、いつでも、どの組み合わせでも相手の会員登録証Ｌを、自分の持っている鍵（ＰｋＴｎ）で確認することができる。

【００８３】次に、チケット署名情報Ｆについて、より詳細に説明する。チケット販売機関Ｂでは、確認鍵ＰｋＢ１，確認鍵ＰｋＢ２，．．．．の順に鍵更新しているものとする。すなわち、前述の会員登録機関Ｔが確認鍵ＰｋＴ１，確認鍵ＰｋＴ２，．．．と更新するのと同様の規則に従って鍵更新を行う。サービス提供者Ｉは、サービス提供保証情報Ｃをチケット販売機関Ｂに登録する。これを契機にして、チケット販売機関Ｂの主鍵・補助鍵を入手する。サービス提供保証情報Ｃ、チケット署名情報Ｆの有効期間は、例えば１年とする。利用者会員Ｕが、チケットを購入する場合、チケット販売機関Ｂは、確認鍵ＰｋＢ３の主鍵ｂ１の署名鍵で、チケット署名情報Ｆ１を生成する。一方、サービス提供者Ｉは、サービス提供保証情報Ｃをチケット販売機関Ｂに登録する際に、チケット販売機関Ｂの確認鍵ＰｋＢ２か、確認鍵ＰｋＢ３のどちらかを入手している（なぜならば、サービス提供保証情報Ｃの有効期間が１年）。また、利用者会員Ｕがチケット署名情報Ｆ１を使用する前に、確認鍵ＰｋＢ４を入手している場合もある。いずれにしても、サービス提供者Ｉは、利用者会員Ｕがチケット署名情報Ｆ１を使用する時点で、確認鍵ＰｋＢ２，確認鍵ＰｋＢ３，確認鍵ＰｋＢ４のいずれかを持っていて、その主鍵か補助鍵のどちらかにｂ１が入っているため、署名確認ができる。

【００８４】また、利用者会員Ｕが、チケットを購入する場合の２つ目の例を挙げる。この場合、チケット販売機関Ｂは、確認鍵ＰｋＢ４の主鍵ｂ２の署名鍵で、チケット署名情報Ｆ２を生成する。一方、サービス提供者Ｉは、サービス提供保証情報Ｃをチケット販売機関Ｂに登録する際に、チケット販売機関Ｂの確認鍵ＰｋＢ３か、確認鍵ＰｋＢ４のどちらかを入手している。また、利用者会員Ｕがチケット署名情報Ｆ１を使用する前に確認鍵ＰｋＢ５を入手している場合もある。いずれの場合にも、サービス提供者Ｉは、利用者会員Ｕがチケット署名情報Ｆ１を使用する時点で、確認鍵ＰｋＢ３，確認鍵ＰｋＢ４，確認鍵ＰｋＢ５のいずれかを持っていて、その主鍵か補助鍵のどちらかにｂ２が入っているため、署名の確認ができる。

【００８５】このように、チケット販売機関Ｂの署名鍵を更新することで、チケット販売機関Ｂが利用者会員Ｕに対して発行する署名Ｆをサービス提供者Ｉは、いつでも確認することができる。

【００８６】

【発明の効果】以上の説明から明らかなように、本発明によれば、署名鍵に用いる鍵を複数個用意し、これらの鍵を一定規則で更新するとともに、確認鍵もこれらの鍵の更新に同期させて更新して公開するようにしたので、更新の際に電子署名の発行を停止させたり、鍵の更新後のサービスの利用を制限する必要がなくなる。また、認証時にオンラインで鍵を取り寄せたり、公開鍵証明書を取得する必要もなくなる。さらに、異なる時期に発行された電子署名の相互認証をオフラインで行うことも可能になった。

【図面の簡単な説明】

【図１】本発明が適用される会員システムの概略構成図。

【図２】図１の構成による鍵等の配送シーケンスを示す手順説明図。

【図３】鍵更新スケジュールの最も単純な例を示したシーケンスチャート。

【図４】周期が変化する場合の鍵更新スケジュールの例を示したシーケンスチャート。

【図５】周期が変化する場合の他の鍵更新スケジュールの例を示したシーケンスチャート。

【図６】５個の鍵を用いる場合の鍵更新スケジュール例を示したシーケンスチャート。

【図７】本発明の鍵管理システムの構成例を示すブロック図。

【図８】（ａ）は鍵管理システムにおける情報処理制御部の詳細ブロック図、（ｂ）はデータファイル装置の詳細構造図。

【図９】本実施形態の会員システムの運用形態を示すブロック図。

【図１０】図９の形態の会員システムにおける鍵配送及び鍵更新の手順説明図。

【図１１】図９の形態の会員システムにおける会員間の相互認証の手順説明図。

【図１２】図９の形態の会員システムにおける会員間の相互認証の手順説明図。

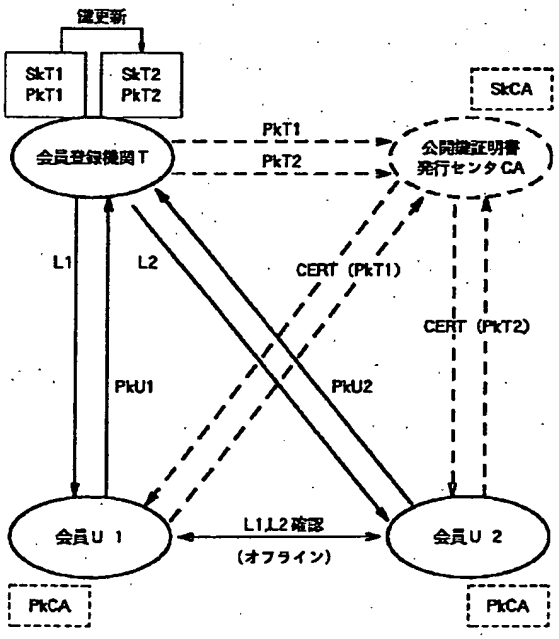
【図１３】本実施形態の他の会員システムの運用形態を示すブロック図。

【図１４】図１３の形態の会員システムにおける鍵更新のスケジュール例を示したシーケンスチャート。

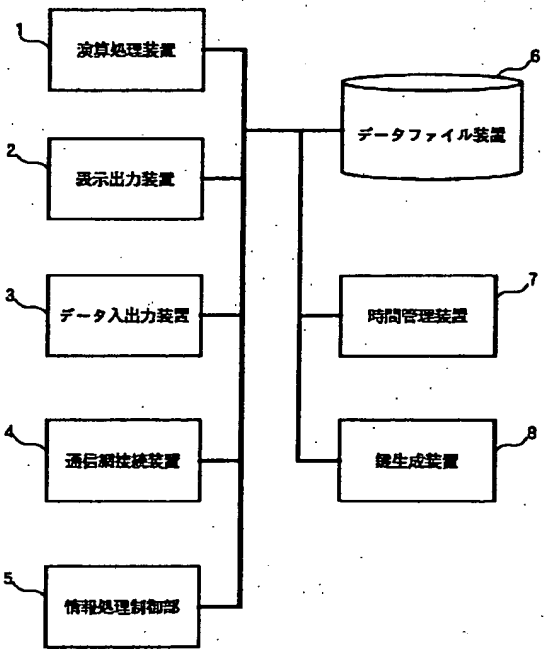
【符号の説明】

1　演算処理装置
2　表示出力装置
3　データ入出力装置
4　通信網接続装置
5　情報処理制御部
6　データファイル装置
7　時間管理装置
8　鍵生成装置

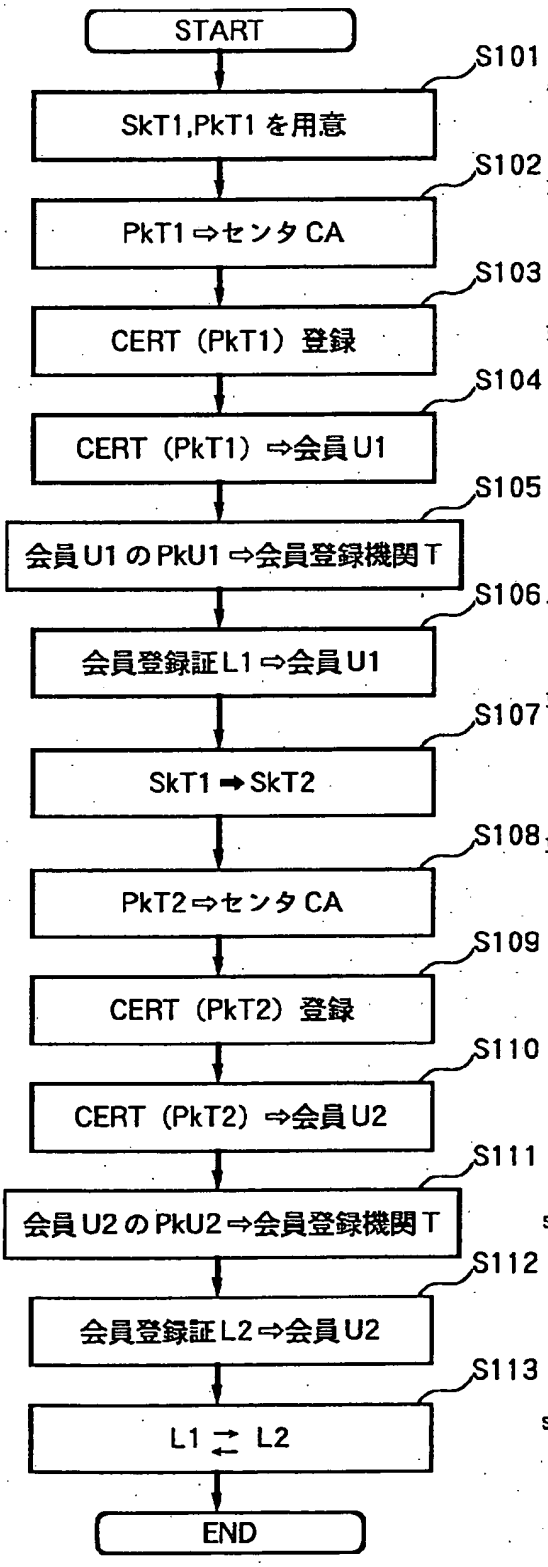
【図１】



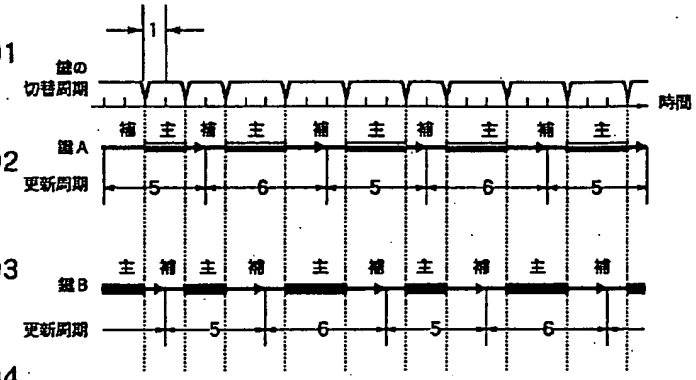
【図７】



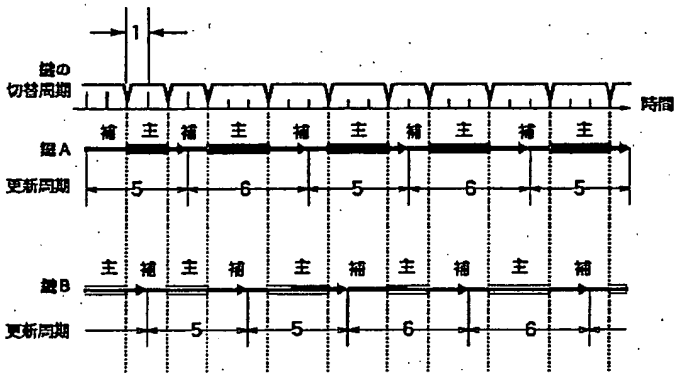
【図２】


START
S101
SkT1,PkT1 を用意
S102
PkT1 ⇨センタ CA
S103
CERT (PkT1) 登録
S104
CERT (PkT1) ⇨会員U1
S105
会員U1 の PkU1 ⇨会員登録機関T
S106
会員登録証L1 ⇨会員U1
S107
SkT1 ➡ SkT2
S108
PkT2⇨センタ CA
S109
CERT (PkT2) 登録
S110
CERT (PkT2) ⇨会員U2
S111
会員U2 の PkU2 ⇨会員登録機関T
S112
会員登録証L2 ⇨会員U2
S113
L1 ⇄ L2
END

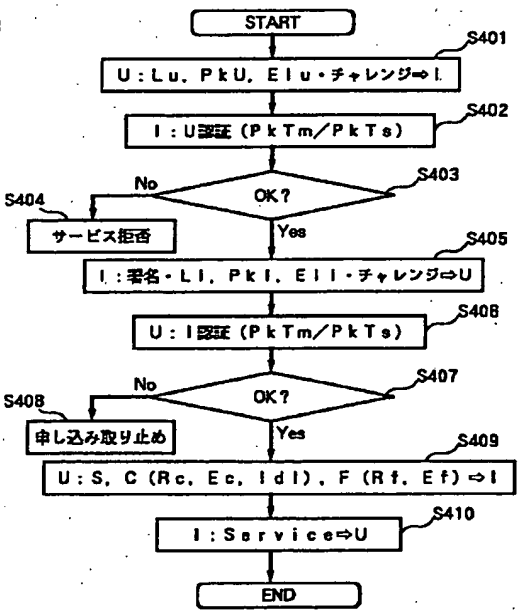
【図４】


1
鍵の切替周期
時間
補 主 補 主 補 主 補 主 補 主
鍵A
更新周期
5 6 5 6 5
主 補 主 補 主 補 主 補 主 補
鍵B
更新周期
5 6 5 6

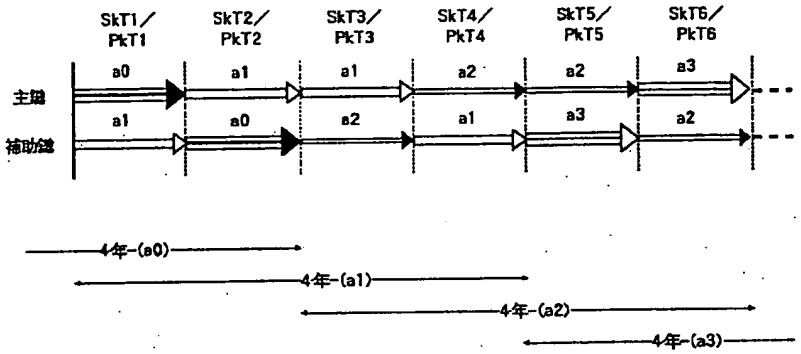
【図５】


1
鍵の切替周期
時間
補 主 補 主 補 主 補 主 補 主
鍵A
更新周期
5 6 5 6 5
主 補 主 補 主 補 主 補 主 補
鍵B
更新周期
5 5 6 6

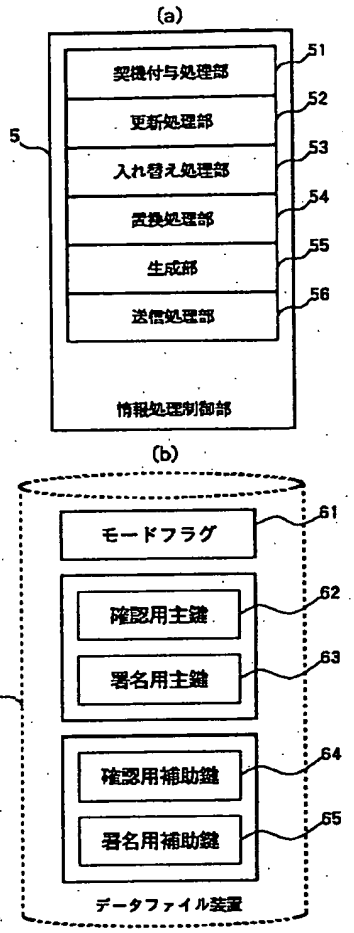
【図１２】


START
S401
U : Lu, PkU, Elu・チャレンジ⇨I
S402
I : U認証 (PkTm/PkTs)
S403
No
OK?
S404
サービス拒否
Yes
S405
I : 署名・LI, PkI, ElI・チャレンジ⇨U
S406
U : I認証 (PkTm/PkTs)
S407
No
OK?
S408
申し込み取り止め
Yes
S409
U : S, C (Rc, Ec, IdI), F (Rf, Ef) ⇨I
S410
I : Service⇨U
END

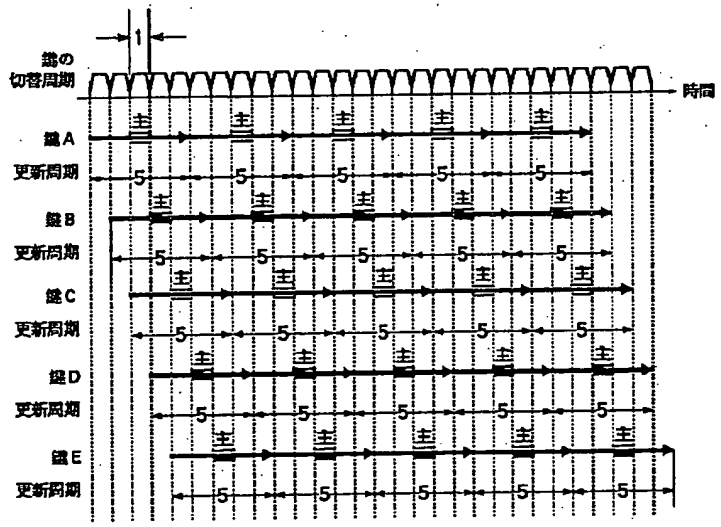
【図３】


SkT1／PkT1
SkT2／PkT2
SkT3／PkT3
SkT4／PkT4
SkT5／PkT5
SkT6／PkT6
主鍵
補助鍵
a0
a1
a2
a3
4年-(a0)
4年-(a1)
4年-(a2)
4年-(a3)

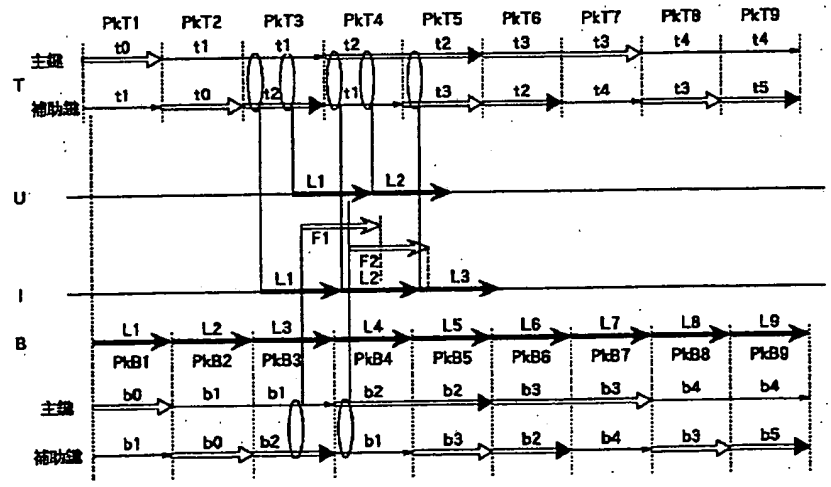
【図８】


(a)
5
契機付与処理部
更新処理部
入れ替え処理部
置換処理部
生成部
送信処理部
情報処理制御部
51
52
53
54
55
56
(b)
6
モードフラグ
確認用主鍵
署名用主鍵
確認用補助鍵
署名用補助鍵
データファイル装置
61
62
63
64
65

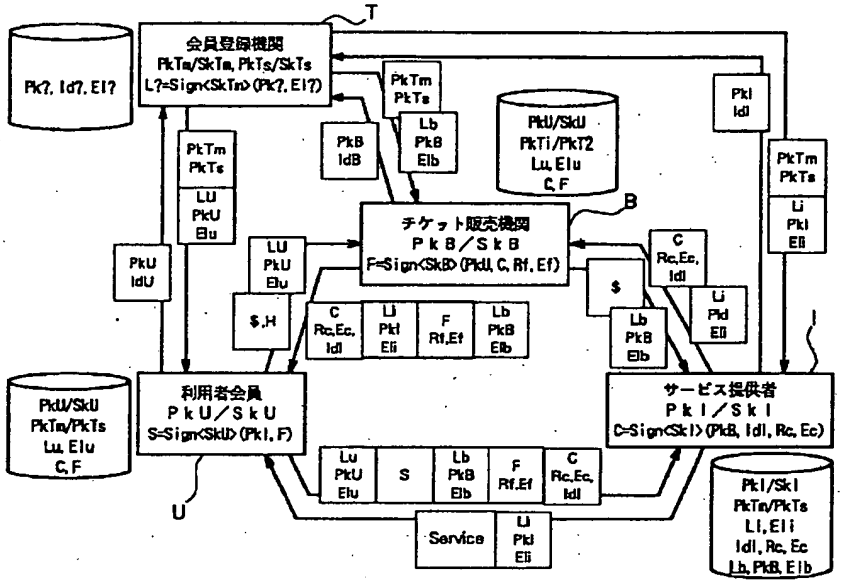
【図６】


鍵の切替周期
1
時間
鍵A
更新周期
鍵B
鍵C
鍵D
鍵E
主
5

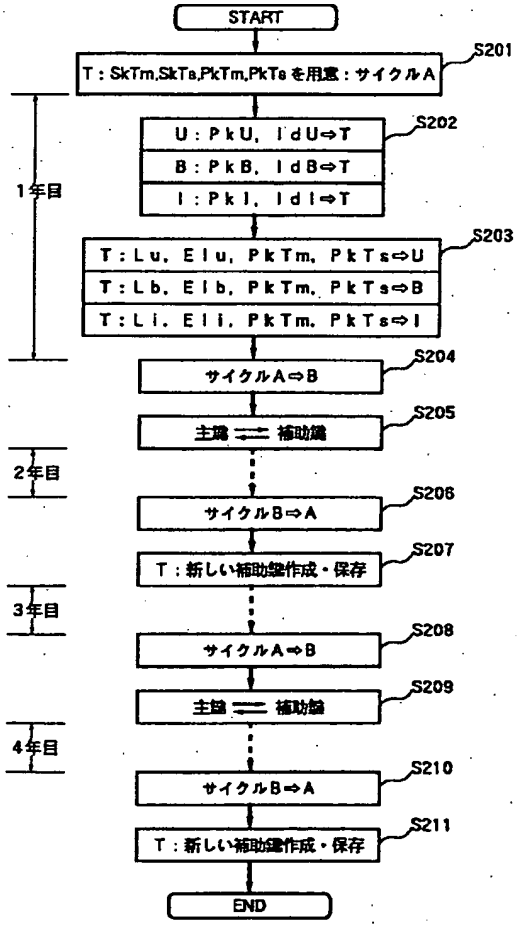
【図１４】


PkT1
PkT2
PkT3
PkT4
PkT5
PkT6
PkT7
PkT8
PkT9
T
主鍵
補助鍵
U
I
B
L1
L2
L3
F1
F2
PkB1
PkB2
PkB3
PkB4
PkB5
PkB6
PkB7
PkB8
PkB9

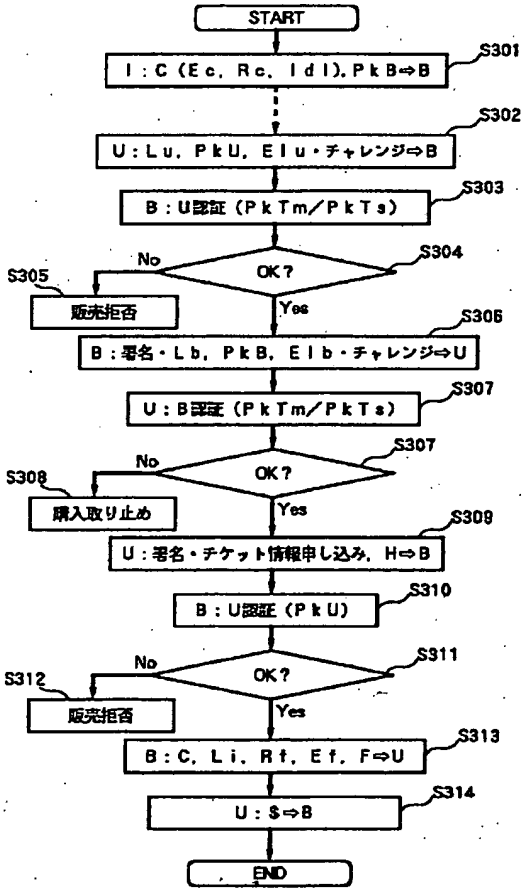
【図９】


T
会員登録機関
PkTa/SkTa, PkTs/SkTs
L?=Sign<SkTa>(Pk?, El?)
Pk?, Id?, El?
PkTm PkTs
PkB IdB
Lb PkB Elb
PkU/SkU PkTi/PkT2 Lu, Elu C, F
PkI IdI
PkTm PkTs
Li PkI Eli
PkTm PkTs
Lu PkU Elu
PkU IdU
Lu PkU Elu
チケット販売機関
P k B／S k B
F=Sign<SkB>(PkU, C, Rf, Ef)
B
C Rc,Ec, Idl
$
Ui PkI Eli
$,H
C Rc,Ec, Idl
Li PkI Eli
F Rf,Ef
Lb PkB Elb
Lb PkB Elb
I
PkU/SkU PkTa/PkTs Lu, Elu C, F
利用者会員
P k U／S k U
S=Sign<SkU>(PkI, F)
サービス提供者
P k I／S k I
C=Sign<SkI>(PkB, IdI, Rc, Ec)
U
Lu PkU Elu
S
Lb PkB Elb
F Rf,Ef
C Rc,Ec, Idl
Service
Ui PkI Eli
PkI/SkI PkTa/PkTs Li, Eli IdI, Rc, Ec Lb, PkB, Elb

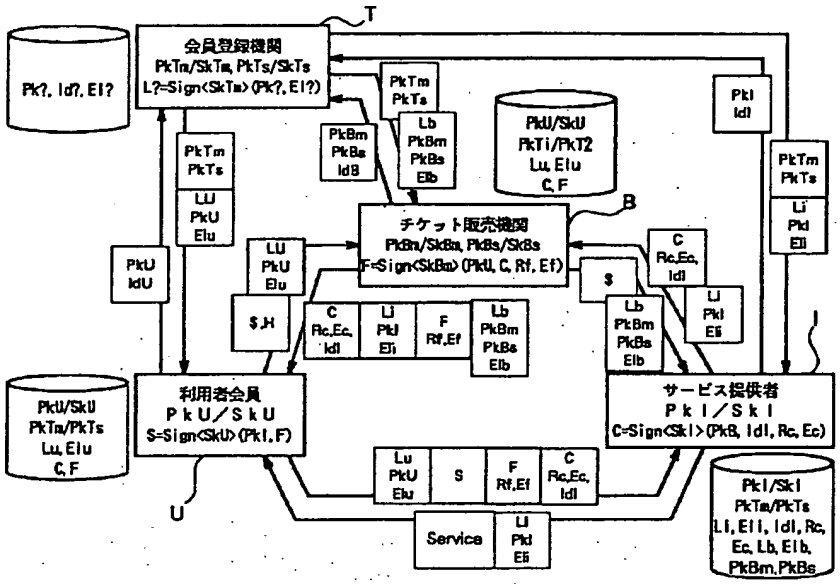
【図１０】


START
T：SkTm,SkTs,PkTm,PkTs を用意：サイクルA
S201
U：P k U, I d U⇒T
B：P k B, I d B⇒T
I：P k I, I d I⇒T
S202
T：Lu, E l u, P k Tm, P k Ts⇒U
T：L b, E l b, P k Tm, P k Ts⇒B
T：L i, E l i, P k Tm, P k Ts⇒I
S203
サイクルA⇒B
S204
主鍵 ⇄ 補助鍵
S205
サイクルB⇒A
S206
T：新しい補助鍵作成・保存
S207
サイクルA⇒B
S208
主鍵 ⇄ 補助鍵
S209
サイクルB⇒A
S210
T：新しい補助鍵作成・保存
S211
END
1年目
2年目
3年目
4年目

【図１１】


START
I：C (E c, R c, I d I), P k B⇒B
S301
U：L u, P k U, E l u・チャレンジ⇒B
S302
B：U認証 (P k Tm／P k Ts)
S303
OK？
S304
No
Yes
S305
販売拒否
B：署名・L b, P k B, E l b・チャレンジ⇒U
S306
U：B認証 (P k Tm／P k Ts)
S307
OK？
S307
No
Yes
S308
購入取り止め
U：署名・チケット情報申し込み, H⇒B
S309
B：U認証 (P k U)
S310
OK？
S311
No
Yes
S312
販売拒否
B：C, L i, R f, E f, F⇒U
S313
U：$⇒B
S314
END

【図１３】



フロントページの続き

(51) Int. Cl. 6	識別記号	ＦＩ
		Ｈ０４Ｌ　9/00　　６０１Ｆ